



U.S. DEPARTMENT OF  
**ENERGY**

**Nuclear Energy**

---

## **Cyber Security R&D (NE-1)**

**Trevor Cook**

**Office of Science and Technology Innovation**

**Office of Nuclear Energy  
U.S. Department of Energy**

# Cyber Security for Nuclear Systems (rapidly evolving environment)

---

- Chatham House Report ““Cyber Security at Civil Nuclear Facilities”, Sep 2015
- Ukraine Power Grid Cyber Attack, Dec 2015
- PDD-41 – “Presidential Policy Directive -- United States Cyber Incident Coordination” July, 2016
- Potential Legislation - S.3018 “Securing Energy Infrastructure Act”
- National Exercises – GridEx III and GridEx IV
- NEI cyber Security Implementation Workshop, March 2016
- INMM Technical Meeting on Nuclear Energy and Cyber Security, April 2016

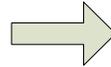


# Implementing Cyber Security

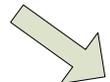
Establish Cyber Security Assessment Team



Establish CSAT



Identify Critical Systems



Identify Digital Devices

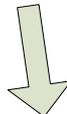
Implement Portable and Mobile Device Controls



Document Findings



Stand up Ongoing Program



Identify CDAs

Implement ongoing program for Cyber Security

Identify Critical Systems and Critical Digital Assets



Remediate CDAs



Assess CDAs

*Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" Guidance for meeting 10 CFR 73.54*

## Objectives:

- **To strength security through reduction of vulnerabilities**
- **To mitigate the consequences of threats**
- **To lower the costs of protection and compliance**
- **To provide a collaborative pathway for industry and researchers**

## Fields of Interest:

- **Risk Management – Architectures and Supply Chain**
- **Modeling & Simulation**
- **Information Sharing/Training/Education**

## NEUP Proposal Interest - R&D Needs

- Enable the current LWR, SMR, Advanced Reactor designs
- Demonstrated increased cybersecurity to facility control systems while maintaining system safety and reliability
- Advance the science and engineering of I&C protocols and/or communication networks that adapt to cyber threat and support inspection and forensics, unique application of intelligent integrated circuits, etc.
- Research should address how the work would be incorporated into an overall secure architecture that can be used by industry and in development of standards for use in nuclear facilities

## Contact Information

---

- For NEUP, interested parties may contact the INL cyber security program manager at [steven.hartenstein@inl.gov](mailto:steven.hartenstein@inl.gov)
- Interested parties may contact me as well at [trevor.cook@nuclear.energy.gov](mailto:trevor.cook@nuclear.energy.gov)